of pregnant females were not included in the averages for their respective age groups. Adult weights will be seen to be essentially alike for the 6- and 12-unit levels, and relatively little higher than for the corresponding animals on the intake level of 3 units per gram. The coefficients of variation of the body weights, as distinguished from gains, were small in all cases.

Much more striking are the facts brought out in the lower section of table 1 which show that in the period of rapid growth, between the 28th and 56th days of the life of these rats, the coefficient of variation of the individual data of the respective groups or series are, in both sexes, much larger for those on the 3 I. U. than for those on the 6- and 12-I. U. levels of vitamin A per gram of food. Yet rat families in our colony are thriving in the 58th generation on the diet containing even the lowest of these three levels.

We conclude that while 3 I. U. of vitamin A per gram of air-dry food (or 0.8 I. U. per food calorie) fully meets the requirements of adequacy, as the word is commonly understood, there is a somewhat higher and a much less variable rate of growth when the level of vitamin A intake is twice or four times higher.

This stabilizing effect appears to be a further advantageous influence of the same liberal levels of dietary vitamin A that have previously been shown[1] beneficial to adult vitality and length of life.

* Aided by grants from The Nutrition Foundation, Inc.

[1] Sherman, H. C., Campbell, H. L., Udiljak, M., and Yarmolinsky, H., these PROCEEDINGS, **31**, 107–109 (1945).

ILLUSTRATIONS AND SIMPLE ABSTRACT PROOF OF SYLOW'S THEOREM

BY G. A. MILLER

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS

Communicated April 30, 1945

Sylow's theorem in the theory of finite groups consists of the following three parts: If the order of a group G is divisible by p^m, p being a prime number, but not by a higher power of p, then G contains at least one subgroup of order p^m, and if it contains more than one such subgroup all of these subgroups are conjugate under G and their number is of the form $1 + kp$. The first of these three parts can be proved independently of the other two parts. In fact, these two parts follow almost directly from the first of these three parts. Hence this part will receive most of our attention in what follows.

A Norwegian mathematician, L. Sylow (1832–1918), was the first to publish this general theorem. It appeared in the French language in a German mathematical journal called *Mathematische Annalen*, **5**, 584–594 (1872). This was about two years after the first treatise on group theory was published by a well-known French mathematician, C. Jordan (1838–1922). The title of this very influential work is *Traité des substitutions et des équations algèbriques* (1870). Various parts of this standard work of XVIII + 667 large pages could have been much simplified by the use of Sylow's theorem if it had then been known. Important steps toward its proof had been taken earlier. In particular, the noted French mathematician, A. L. Cauchy (1789–1857), published a proof of the fact that if the order of a group is divisible by a prime number then the group contains a subgroup whose order is equal to this number and hence the theorem has often been called the Cauchy-Sylow theorem. This special case had been stated without proof by E. Galois (1811–1832).

When G is an abelian group it can be proved very easily that Sylow's theorem applies to it by using the following obvious theorem relating to the order of the product of two commutative group operators. This order is the product of all the powers of the prime numbers which appear to a higher power in the order of one of these two operators then in the order of the other and the product of divisors of powers of prime numbers appearing to the same highest powers in the orders of the two given operators. The same theorem may be expressed by saying that if p^α is the highest power of p which divides the order of one of the two given operators but is not a divisor of the order of the other then it is a divisor of the order of their product but if p^α is the highest power of p which divides the orders of both of these operators and neither of them is divisible by a higher power of p then the order of their product is divisible by no higher power of p than p^α. The product of all such powers of prime numbers is the order of the product of the two given group operators.

From this theorem it follows directly that if none of the operators of the abelian group G has an order which is divisible by p then the order of G cannot be divisible by p and if the order of such an operator of G is divisible by p this operator is the product of an operator whose order is a power of p and an operator, which may be the identity, whose order is prime to p. Hence all the operators of G may be supposed to be so represented that some of them have orders which are powers of p while the rest of them have orders which are prime to p. The former will therefore generate a subgroup whose order is a power of p while the latter generate a subgroup whose order is prime to p and G is the direct product of these two subgroups. The order of the former subgroup is the highest power of p which divides the order of G and this is therefore the Sylow subgroup of order p^m contained in G.

It remains to consider the case when G is non-abelian, and it may first be noted that it may be assumed that G is one of the non-abelian groups of smallest order to which Sylow's theorem does not apply in case it does not apply to G. If G contains more than one invariant operator all of its invariant operators generate an invariant subgroup of G. Since both the order of this subgroup and the order of the corresponding quotient group are smaller than that of G it follows that Sylow's theorem applies to both of them and hence it also applies to G, which is contrary to the stated hypothesis. It therefore follows that it may be assumed that the identity is the only invariant operator of G.

All the operators of G can be arranged in sets of conjugates such that no two sets have any operator in common and that the identity alone constitutes one of these sets. Each of the operators of one of the sets is transformed into itself by all the operators of a subgroup of G and the number of the operators in the set is equal to the order of G divided by the order of a subgroup of G. Hence there results the following equation:

$$g = 1 + g_1 + g_2 + \ldots + g_n.$$

In this equation g represents the order of G and $g_1, g_2, \ldots, g_n$ represent the numbers of the operators in the given sets of conjugates. It should be noted that each of the numbers $g_1, g_2, \ldots, g_n$ usually exceeds unity and is equal to g divided by the order of a subgroup of G.

Since p divides g it cannot divide each of the numbers $g_1, g_2, \ldots, g_n$. Hence there is at least one of these numbers which is prime to p and each of the corresponding subgroups must have a common order which is divisible by p^m. These subgroups are found in G and hence G contains a subgroup of order p^m. To prove that all the subgroups of order p^m in G form a single set of conjugates it may be noted that a given one of these subgroups could not transform into itself another one of them since g is not divisible by a higher power of p than p^m. Therefore it results that if there were more than one set of such subgroups it would follow that if those of a set were transformed by one of their conjugates the number of the subgroups in the set would be of the form $1 + kp$ and if those of the same set were transformed by one of those in another set of conjugates this number would have to be of the form kp. Since this is a contradiction it has been proved that all these subgroups of order p^m are conjugate under G and that their number is of the form $1 + kp$.

The equation

$$g = 1 + g_1 + g_2 + \ldots + g_n$$

is fundamental. When $n = 1$, G is obviously the group of order 2. When

$n = 2$ G is either the group of order 3 or the symmetric group of order 6. When G is any abelian group n is clearly equal to $g - 1$ and hence it is only necessary to consider the cases when G is non-abelian. In all of these cases n is less than $g - 1$ and at least equal to the number of the distinct prime numbers which divide g. If it is equal to this number g cannot be divisible by the square of a prime number and hence it contains then an invariant subgroup whose order is the largest prime number which divides g. Hence the symmetric group of order 6 is the only group in which n is no larger than the number of the distinct prime numbers which divide g when G is a non-abelian group.

For every prime divisor p of g there is at least one of the numbers g_1, g_2, ..., g_n which is prime to p and the sum of all such numbers when this sum is increased by unity is divisible by p. This includes the well-known theorem that every group of order p^m contains at least $p - 1$ invariant operators besides the identity, since the number of the operators in every set of conjugates of such a group is divisible by p whenever the set contains more than one operator. Hence the formula $g = 1 + g_1 + g_2 + \ldots + g_n$ which is useful in proving Sylow's theorem is also useful in the study of the prime power groups. A necessary and sufficient condition that G is an abelian group is that each of the numbers g_1, g_2, ..., g_n is unity and hence n has then its maximal value.

When G is non-abelian the maximal value of n will clearly result when the number of the invariant operators of G is as large as possible and each of the non-invariant operators of G has only two conjugates under G provided that both of these conditions can be satisfied at the same time. This can be done in the present case. In fact, the largest number of the invariant operators of a non-abelian group can clearly not exceed the order of the group divided by 4 and when it is equal to this number the commutator subgroup of the group is of order 2 and hence each of the non-invariant operators of G has exactly two conjugates under G. In other words, when G is a non-abelian group the maximal value of n is $5g/8 - 1$ and the central of G is of order $g/4$ while its commutator subgroup is of order 2. The octic group is clearly the smallest group which satisfies these conditions.

A necessary and sufficient condition that the non-abelian group G contains a maximal number of sets of conjugate operators is that it contains three abelian subgroups of index 2. If it contains two such subgroups it also contains three such subgroups and its central is of index 4 under G while its commutator subgroup is of order 2. The theorem that a non-abelian group has three, one, or no abelian subgroups of index 2 is a special case of the theorem that a non-abelian group of order p^m has $p + 1$, one, or no abelian subgroup of index p, where p is a prime number. If a non-abelian group of order p^n contains more than one abelian subgroup of

index p the number of its sets of conjugate operators is $p^{m-2} + p^{m-1} - p^{m-3}$ and hence the maximal value of n in this case is $p^{m-3}(p^2 + p - 1) - 1$. This evidently reduces to $5g/8 - 1$ when $p = 2$ as was noted above.

ON THE NUMBER OF SOLUTIONS OF CERTAIN NON-HOMOGENEOUS TRINOMIAL EQUATIONS IN A FINITE FIELD

BY H. S. VANDIVER

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF TEXAS

Communicated May 7, 1945

The relation

$$au^m + bv^m + 1 = 0, \tag{1}$$

where a and b are given elements of a finite field F, with u and v to be determined in F, with $abuv \neq 0$, has been studied by Mitchell.[1] For the special case where F consists of residue classes with respect to a prime modulus, this equation has been studied by a number of writers.[2] All the methods used by these writers appear to depend on a certain symmetry arising from the fact that the exponents of u and v are the same.

However, in another paper[3] the writer obtained, based mainly on extensions of a method due to V. A. Lebesgue,[4] an expression for the number of roots of equation (1) modulo p which was independent of this symmetry. Hence, we shall apply this latter method to the consideration of

$$au^e + bv^f + w^g = 0 \tag{1a}$$

and

$$au^e + bv^f + 1 = 0. \tag{1b}$$

We shall find expressions for the number of solutions (u^e, v^f, w^g) of equation (1a) and the number of solutions (u^e, v^f) of equation (1b) in a finite field F, providing that $abuvw \neq 0$. If we obtain this number, then we may immediately find the number of solutions (u, v, w). Also we may confine ourselves to the case where e, f and g are divisors of $p^n - 1$, where the order of F is p^n, when p is prime, as the other cases depend on this.

Using Theorem II of my previous paper,[3] we determine N in the relation

$$N = \sum(1 - (ax_1 + bx_2 + x_3)^{p^n-1}), \tag{2}$$

when the summation extends over x_1, x_2, x_3, where x_1 ranges independently over all the distinct values such that $x_1^h = 1$, similarly x_2 over all roots of $x_2^i = 1$, and x_3 over all roots of $x_3^j = 1$, where